BAE SYSTEMS

Federal Supply Service Authorized Schedule 84 Pricelist

Total Solutions for Security, Facility Management Systems, and Emergency/Disaster Response

GSA Schedule No: GS-07F-0077X
Contract Period: 10/21/2010-10/20/2015
Business Size: Large
Current through: Mod PO-0004 dated 08/03/2011

246-60-1-Security Systems Integration and Design Services

Services involving the security integration and/or management discipline which supports security products or systems through their life cycle. Security Systems integration and design services may include, but are not limited to those associated with the design, test, production, fielding, sustainment, improvement of cost effective security and/or protection systems including the eventual disposal or salvage of these systems. Services may include studies and analysis such as - risk assessment, threat evaluation, and assessment (including resultant deliverables). Contractors may provide security or protection expertise in the pre-production or design phase of security or protection systems to ensure that the system can be supported through its life-cycle and that the infrastructure elements necessary for operational support are identified and acquired. These services may continue through the life cycle of the system or product and may include guidance, assistance and/or operational support. This includes all necessary security management elements.

246-60-2-Security Management and Support Services

Services providing the best practices, technologies and methodologies to plan, design, manage, operate and maintain secure and protected systems, equipment, facilities and infrastructures. Agency orders may include complete turnkey operations, maintenance and support services, or components thereof as needed to ensure secure and protected systems involving personnel security, physical access, and information security, and reduce life cycle costs. Contractor personnel carrying out these activities, to include management and operating staffs, are not involved with or responsible for the core business of the customer agency placing the order.

246-60-3-Security System Life Cycle Support Services

Services providing for design, coding, integration, testing, deploying, repair and maintenance of integrated security systems, and training across all platforms, enterprise wide, for the complete life cycle of the system.

SIN 246-52: Security Consulting/Training and Facility Management Consulting. Professional Services offered under this SIN shall be for the support of security systems (including access control, intrusion alarms, fire alarm systems, etc.) and Facility Management Systems (including security and energy management) only. Excludes personal services.

BAE Systems Information Solutions Inc.
2525 Network Place
GSA/GWAC Acquisition Center
Herndon, Virginia 20171
Gsa.it.pmo@baesystems.com

Product and ordering information in this authorized schedule pricelist is also available on the GSA Advantage! Agencies can browse GSA Advantage! by accessing GSA's Home Page via Internet at www.gsa.gov.

Table of Contents

Information for Ordering Offices

Special Notice to Agencies: Small Business Participation

SBA strongly supports the participation of small business concerns in the Federal Supply Schedules Program. To enhance Small Business Participation SBA policy allows agencies to include in their procurement base and goals, the dollar value of orders expected to be placed against the Federal Supply Schedules, and to report accomplishments against these goals.

For orders exceeding the micropurchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelists of at least three schedule contractors or consider reasonably available information by using the GSA Advantage!™ on-line shopping service (www.fss.gsa.gov). The catalogs/pricelists, GSA Advantage!™ and the Federal Supply Service Home Page (www.fss.gsa.gov) contain information on a broad array of products and services offered by small business concerns.

This information should be used as a tool to assist ordering activities in meeting or exceeding established small business goals. It should also be used as a tool to assist in including small, small disadvantaged, and women-owned small businesses among those considered when selecting pricelists for a best value determination. For orders exceeding the micropurchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy their requirement.

1. Geographic Scope of Contract

Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

Overseas delivery is delivery to points outside of the 48 contiguous states, Washington, DC, Alaska, Hawaii, Puerto Rico, and U.S. Performance in the following countries to include but not limited to Africa, Europe (all countries within), Iraq, and Korea.

Offerors are requested to check one of the following boxes:

[X] The Geographic Scope of Contract will be domestic and overseas delivery.
[ ] The Geographic Scope of Contract will be overseas delivery only.
[ ] The Geographic Scope of Contract will be domestic delivery only.

2. Contractor's Ordering Address and Payment Information

Contractor: BAE Systems Information Solutions Inc. (www.bae-it.na.baesystems.com)

Ordering point of contact: Tel.: 703-563-7980; Fax: 703-563-7702
gsa.schedules.pmo@baesystems.com

Ordering address: BAE Systems Information Solutions Inc.
GSA/GWAC Acquisition Center
2525 Network Place
Herndon, VA 20171

Payment address: Citibank Delaware
One Penn's Way
New Castle, DE 19702

Tax ID number: 54-1168311

DUNS number: 00-464-9125

Cage code (FSCM): 0GS16

GSA Contracts Manager	Sr. Contracts Lead
Thelma Miles BAE Systems Information Solutions, Inc. GSA/GWAC Acquisition Center 28525 Network Place Herndon, VA 20171 Tel.: 703-563-7704; Fax: 703-563-7702	Jeffrey Kozak BAE Systems Information Solutions, Inc. GSA/GWAC Acquisition Center 2525 Network Place Herndon, VA 20171 Tel.: 703-563-7980; Fax: 703-563-7702

Ordering points of contact, ordering address, and payment information for authorized BAE Systems locations appear below:

Authorized Reseller	Ordering Point of Contact	Ordering Address	Payment Address	Tax ID Number	DUNS Number	Cage Code (FSCM)
BAE Systems Goespatial Products & Solutions, Inc.	Ian MacLaren 856-793-4293 fax: 856-866-7800	BAE Systems GPS 124 Gaither Drive Suite 100 Mount Laurel, NJ 08054	BAE Systems GPS 124 Gaither Drive Suite 100 Mount Laurel, NJ 08054	33-0536290	79-703-2372	2N028
BAE Systems National Security Systems, Inc.	Joan Lachowicz 402-827-5806 fax: 402-827-0550	BAE Systems National Security Solutions, Inc. 1410 Wall Street Bellevue, NE 68005	BAE Systems National Security Systems, Inc. c/o Citibank Delaware PO Lockbox 7247-6941 Philadelphia, PA 19170-6941	33-0536290	03-983-2233	0H0J7
BAE Systems National Security Systems, Inc.	Bill Wulff 858-592-5884 fax: 858-675-5878	BAE Systems National Security Systems, Inc. 10920 Technology Pl. San Diego, CA 92127	BAE Systems National Security Systems, Inc. c/o Citibank Delaware PO Lockbox 7247-6941 Philadelphia, PA 19170-6941	33-0536290	79-703-2372	12436
BAE Systems Technology Solutions and Services Inc.	Terri Rushing 256-890-8098 fax: 256-319-4098	BAE Systems Technology Solutions and Services Inc. 1601 Research Blvd. Rockville, MD 20850-3173	BAE Systems Technology Solutions and Services Inc. P.O. Box 64528 Baltimore, MD 21264	22-2466421	10-393-3453	99789

3. Liability for Injury or Damage

The contract shall not be liable for any injury to Government personnel or damage to Government property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

4. Statistical Data for Government Ordering Office Completion of Standard Form 279

Block 9: G. Order/Modification Under Federal Schedule
Block 16: Contractor Establishment Code (DUNS): See relevant contractor ordering information or reseller information in paragraph 2 above.
Block 30: Type of Contractor – C. Large Business
Block 31: Woman-Owned Small Business – No
Block 36: Contractor's Taxpayer Identification Number (TIN): See relevant contractor or reseller ordering information in paragraph 2 above.

4a. CAGE Code

See relevant contractor or reseller ordering information.

5. FOB-N/A

6. Delivery Schedule

(a) TIME OF DELIVERY. The Contractor shall deliver to destination 30 days after receipt of order, or as negotiated between Government and the Contractor.

(b) URGENT REQUIREMENTS. When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering agency, agencies are encouraged, if time permits, to contact the contractor for the purpose of obtaining accelerated delivery. The contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the contractor in writing.) If the contractor offers an accelerated delivery time acceptable to the ordering agency, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

7. Discounts

Prices shown are net prices; basic discounts have been deducted.

a. Prompt Payment: 0% Net 30 days
b. Quantity: 3% discount on individual task orders over $20,000,000.00
c. Dollar Volume: 3% discount on individual task orders over $20,000,000.00
d. Government Educational Institutions: None
e. Other: None

8. Trade Agreements Act of 1979, As Amended

All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.

9. Statement Concerning Availability of Export Packing

Not within the scope of the contract.

10. Minimum Order

The minimum dollar value of orders to be issued is $100.

11. Maximum Order

SPECIAL ITEM 246-60-1 – Security Systems Integration and Design Services
The maximum dollar value per order: $200,000

SPECIAL ITEM 246-60-2 – Security Management and Support Services
The maximum dollar value per order: $200,000

SPECIAL ITEM 246-60-3 – Security Systems Life Cycle Support
The maximum dollar value per order: $200,000

12. Security Requirements

In the event security requirements are necessary, the ordering activities may incorporate, in their delivery order(s), a security clause in accordance with current laws, regulations, and individual agency policy; however, the burden of administering the security requirements shall be with the ordering agency. If any costs are incurred as a result of the inclusion of security requirements, such costs will not exceed ten percent (10%) or $100,000, of the total dollar value of the order, whichever is lesser.

13. Contract Administration For Ordering Offices

Any ordering office, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (1) Termination for the Government's Convenience, and (m) Termination for Cause (See C.1.).

14. GSA Advantage!

The GSA Advantage! is an on-line, interactive electronic information and ordering system that provides on-line access to vendors' schedule pricelists with ordering information. GSA Advantage! will allow the user to perform various searches across all contracts including, but not limited to:

(1) Manufacturer;
(2) Manufacturer's part number; and
(3) Product categories.

Agencies can browse GSA Advantage! by accessing the Internet World Wide Web utilizing a browser (example: Netscape). The Internet address is http://www.fss.gsa.gov .

15. Purchase of Incidental, Non-Schedule Items

NOTE: Open Market Items are also known as incidental items, noncontract items, non-Schedule items, and items not on a Federal Supply Schedule contract. ODCs (Other Direct Costs) are not part of this contract and should be treated as open market purchases. Ordering Activities procuring open market items must follow FAR 8.401(d).
For administrative convenience, an ordering activity contracting officer may add items not on the Federal Supply Multiple Award Schedule (MAS) -- referred to as open market items -- to a Federal Supply Schedule blanket purchase agreement (BPA) or an individual task or delivery order, only if –

(1) All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed (e.g., publicizing (Part 5), competition requirements (Part 6), acquisition of commercial items (Part 12), contracting methods (Parts 13, 14, and 15), and small business programs (Part 19));

(2) The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;

(3) The items are clearly labeled on the order as items not on the Federal Supply Schedule; and

(4) All clauses applicable to items not on the Federal Supply Schedule are included in the order.

16. Contractor Commitments, Warranties and Representations

(a) For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:
  (1) Time of delivery/installation quotations for individual orders;
  (2) Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/ service/software package submitted in response to requirements which result in orders under this schedule contract.
  (3) Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the contractor.
(b) The above is not intended to encompass items not currently covered by the GSA Schedule Contract.

17. Overseas Activities

The terms and conditions of this contract shall apply to all orders for services in areas listed in the pricelist outside the 48 contiguous states and the District of Columbia, except as indicated below:

Not Applicable

Upon request of the contractor, the Government may provide the contractor with logistics support, as available, in accordance with all applicable Government regulations. Such Government support will be provided on a reimbursable basis, and will only be provided to the contractor's technical personnel whose services are exclusively required for the fulfillment of the terms and conditions of this contract.

18. Blanket Purchase Agreements (BPAs)

Federal Acquisition Regulation (FAR) 13.303-1(a) defines Blanket Purchase Agreements (BPAs) as "…a simplified method of filling anticipated repetitive needs for supplies or services by establishing 'charge accounts' with qualified sources of supply." The use of Blanket Purchase Agreements under the Federal Supply Schedule Program is authorized in accordance with FAR 13.303-2(c)(3), which reads, in part, as follows:

"BPAs may be established with Federal Supply Schedule Contractors, if not inconsistent with the terms of the applicable schedule contract."

Federal Supply Schedule contracts contain BPA provisions to enable schedule users to maximize their administrative and purchasing savings. This feature permits schedule users to set up "accounts" with Schedule Contractors to fill recurring requirements. These accounts establish a period for the BPA and generally address issues such as the frequency of ordering and invoicing, authorized callers, discounts, delivery locations and times. Agencies may qualify for the best quantity/volume discounts available under the contract, based on the potential volume of business that may be generated through such an agreement, regardless of the size of the individual orders. In addition, agencies may be able to secure a discount higher than that available in the contract based on the aggregate volume of business possible under a BPA. Finally, Contractors may be open to a progressive type of discounting where the discount would increase once the sales accumulated under the BPA reach certain prescribed levels. Use of a BPA may be particularly useful with the new Maximum Order feature. See the Suggested Format, contained in this Schedule Pricelist, for customers to consider when using this purchasing tool.

19. Contractor Team Arrangements

Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Industrial Funding Fee and Sales Reporting, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

20. Acceptance of Government Purchase Card

Government Commercial Purchase Credit Cards will be acceptable for payment. Information for wire transfer will be contained on invoices.

21. Prime Contractor Ordering From Federal Supply Schedules

Prime Contractors (on cost reimbursement contracts) placing orders under Federal Supply Schedules per FAR Subpart 51 (JAN 2010), on behalf of an ordering activity, shall follow the terms of the applicable schedule and authorization and include with each order:

(a) A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and

(b) The following statement: "This order is placed under written authorization from _____ dated _____. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern."

22. Insurance—Work On A Government Installation (JAN 1997) (FAR 52.228-5)

(a) The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.

(b) Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an

endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective —

(1) For such period as the laws of the State in which this contract is to be performed prescribe; or

(2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance, and shall make copies available to the Contracting Officer upon request.

23. Section 508

If applicable, Section 508 compliance information for Electronic and Information Technology (EIT) supplies and services will be addressed on a task order by task order basis. The EIT standards can be found at www.Section508.gov.

24. GSAR 552.216-70 Economic Price Adjustment-FSS Multiple Award Schedule Contracts

Current pricelist reflects a 12 month period as per GSA. BAE Systems will negotiate years 2011 through 2015 as per the above referenced GSAR clause and reserves the right to escalate labor rates in accordance with GSA contracting Officer's review and approval.

Labor Category Descriptions

1. Program Manager

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 12 years of ADP experience, including at least 8 years of ADP and/or telecommunications system management experience.

Specialized Experience: At least 8 years of direct supervision of ADP software development, integration, maintenance projects, and/or telecommunications systems. Must be capable of leading projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analyzing, designing, integrating, testing, documenting, converting, extending, and implementing automated information and/or telecommunications systems. Must have proven skills that are specified in the delivery order to be managed.

Duties: Performs day-to-day management of overall contract support operations, possibly involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Demonstrates written and oral communications skills. Establishes and alters (as necessary) the corporate management structure to direct effective contract support activities. Must be capable of negotiating and making binding decisions for the company.

2. Project Manager

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 10 years of ADP or telecommunications experience, including at least 5 years of ADP software management experience.

Specialized Experience: At least 5 years of direct supervision of ADP software development, integration maintenance projects, and/or telecommunications management experience.

Duties: Performs day-to-day management of assigned delivery orders/projects that involve teams of data processing and other information systems/management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, converting, extending, and implementing automated information and telecommunications systems and solutions. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. Organizes, directs, and coordinates the planning and production of all activities associated with assigned delivery order projects. Demonstrates written and oral communications skills.

3. Software/Integration Analyst

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 8 years of progressive working experience, including 5 years of specialized experience.

Specialized Experience: At least 5 years of experience as a computer systems analyst.

Duties: Must be knowledgeable in implementing computer systems in a phased approach of requirements analysis and conceptual design, site survey, system design review, installation, integration, and testing. Must be knowledgeable in performing requirements analysis for a wide range of users in areas, including

Year 2000, Electronic Data Interchange (EDI), office automation, web browser design and development, management information systems, weapons systems, and/or finance and accounting. Must be able to present system designs for user approval at formal reviews. Must be capable of performing configuration management, integrating software, interpreting software test results, and recommending solutions for unsatisfactory test results. Must be knowledgeable in lifecycle support, including maintenance, administration, and management.

4. Subject Matter Expert 1

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 6 years of experience in the ADP field, including 4 years of specialized experience.

Specialized Experience: At least 4 years of combined new and related older technical experience in the ADP field directly related to the required area of expertise.

Duties: Develops requirements from a project's inception to conclusion in the subject matter area, for simple to moderately complex systems. Assists other staff with analysis, evaluation and the preparation of recommendations for systems improvements, optimization, development, and/or maintenance efforts in any of the following specialties:

a. Information Systems Architecture
b. Networking
c. Telecommunications
d. Automation
e. Communications Protocols
f. Electronic Mail (E-mail)
g. Internet (Web Technologies)
h. Risk Management/Electronic Analysis
i. Software [consisting of all commercially available software used under this contract for personal computers (PCs), minis, and mainframes]
j. Lifecycle Management
k. Software Development Methodologies
l. Modeling and Simulation
m. Graphics Processing
n. Data Warehousing.

5. Subject Matter Expert 2

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 10 years of experience in the ADP field, including 6 years of specialized experience.

Specialized Experience: At least 6 years of combined new and related older technical experience in the ADP field directly related to the required area of expertise.

Duties: Defines the problems and analyzes and develops plans and requirements in the subject matter area for moderately complex to complex systems. Coordinates and manages the preparation of analysis, evaluations, and recommendations for proper implementation of programs and systems specifications in any of the following specialties:

a. Information Systems Architecture

b. Networking
c. Telecommunications
d. Automation
e. Communications Protocols
f. Electronic Mail
g. Internet (Web Technologies)
h. Risk Management/Electronic Analysis
i. Software (consisting of all commercially available software used under this contract for PCs, minis, and mainframes)
j. Lifecycle Management
k. Software Development Methodologies
l. Modeling and Simulation
m. Graphics Processing
n. Data Warehousing

6. Process Re-engineering Specialist 1

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have a minimum of 8 years of experience, at least 5 years of which must be specialized.

Specialized Experience: At least 5 years of experience, which may include facilitation, training, methodology development and evaluation, process reengineering across all phases, identification of best practices, change management, business management techniques, organizational development, activity and data modeling, or information system development methods and practices and supervision of other staff.

Duties: Applies process improvement and reengineering methodologies and principles to conduct process modernization projects. Duties include activity and data modeling, developing modern business methods, identifying best practices, and creating and assessing performance measurements. Provides group facilitation, interviewing, and training, and provides additional forms of knowledge transfer. May be under the supervision and direction of a principal business process reengineering specialist or may work independently

7. Process Re-engineering Specialist 2

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have a minimum of 10 years of experience, at least 7 years of which must be specialized

Specialized Experience: At least 7 years of experience, which may include facilitation, training, methodology development and evaluation, process reengineering across all phases, identification of best practices, change management, business management techniques, organizational development, activity and data modeling, or information system development methods and practices and supervision of business process reengineering specialist.

Duties: Applies process improvement and reengineering methodologies and principles to conduct process modernization projects. Responsible for effective transitioning of existing project and project teams, and facilitating project teams in the accomplishment of project activities and objectives. Provides group facilitation, interviewing, and training, and provides additional forms of knowledge transfer. Key coordinator among multiple project teams to ensure enterprise-wide integration of reengineering efforts. Provides daily supervision and direction to business process reengineering specialist.

8. Computer Specialist 1

Education: B.A. or B.S. degree, or equivalent experience in a related field.
General Experience: Must have 1 year of computer experience in at least two of the following disciplines: systems analysis, systems programming, application programming, or equipment analysis. General experience and specialized experience may have been accomplished in tandem.

Specialized Experience: At least 1 year of experience in evaluating state-of-the-art computer hardware and software and its ability to support specific requirements.

Duties: Participates in the evaluation of state-of-the-art computer hardware and software and assessment of its ability to support specific requirements and interface with other equipment and systems; determines potential and actual bottlenecks, and proposes recommendations for their elimination; and recommends systems improvements that will result in optimization of development and/or maintenance efforts.

9. Computer Specialist 2

Education: B.A. or B.S degree or equivalent experience in a related field.
General Experience: Must have 4 years of computer experience, including 2 years of specialized experience.

Specialized Experience: At least 2 years of experience as either a computer hardware and/or systems software specialist, or as a systems analyst with duties relating to the evaluation of third- and fourth-generation or state-of-the-art computer hardware and software and its ability to support specific requirements for systems management or large-scale system development and maintenance.

Duties: Must be able to determine costs for converting computer systems from one language or machine to another by utilizing compilers, simulators, emulators, and/or language translators and recommend better utilization of operating systems capabilities to improve system efficiency through conversion or migration. Must be able to develop, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements and interface with other equipment and systems; determine potential and actual bottlenecks, and propose recommendations for their elimination; and recommend systems improvements that will result in optimal hardware and software usage.

10. Project Control 1

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 3 years of financial management experience, including 1 year of specialized experience.

Specialized Experience: At least 1 year of experience in Government financial fee-for-services environment that incorporates financial processes into automated systems.

Duties: Must be able to determine the feasibility of automating Government financial business practices. Defines governmental financial business practices and Electronic Commerce/Electronic Data Interchange (EC/EDI) opportunities, and incorporates the defined processes into an automated solution that includes relational databases and distributed systems. Must be able to either recommend functional requirements for applications to be developed or justify the nondevelopment based on either cost or technology nonavailability. Communicates with both ADP and financial-oriented individuals to document the flow, recommend

opportunities, impact recommendations, and serve as the liaison between the financial specialist and automation specialist that do not have both disciplines.

11. Project Control 2

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 6 years of financial management experience, including 3 years of specialized experience.

Specialized Experience: At least 3 years of experience in financial management with demonstrated ability in analyzing, designing, and developing automated applications for unique business practices in a fee-for-services environment.

Duties: Must be able to clearly define Government financial business practices for integration into the Government financial business system. Identifies potential problems and solutions through analysis, identifying recommended solutions. Works with contractors, vendors, and customers to effectively integrate the customer's requirements into an automated application. Acts as a focal point to coordinate all disciplines in the recommended solution. Applies state-of-the-art applications that will effectively automate financial applications.

12. Project Control 3

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 10 years of financial management experience, including 5 years of specialized experience.

Specialized Experience: At least 5 years of experience in financial management with demonstrated ability to supervise or lead a team of analysts.

Duties: Serves as a group or task leader, ensuring that group analysts are working in concert to automate complex business practices within the timeframe specified by the customer and that all of the requirements are met. Must be able to assess products and procedures for compliance with Government standards, accounting principles, and multi-tiered system application standards. Must be able to grasp interrelationships between financial management requirements and automation solutions, considering the current system environment, and the potential integration of added systems concurrently or later. Prepares milestone status reports and presentations for colleagues, subordinates, and end user representatives.

13. Systems Analyst 1

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 1 year of computer experience in assignments of a technical nature working under close supervision and direction. General experience and specialized experience may have been accomplished in tandem.

Specialized Experience: At least 1 year of experience in analyzing and programming applications on large-scale or mid-tier (or LAN-based) computers, including design and programming of moderately complex ADP systems.

Duties: Develops requirements for information systems from a project's inception to its conclusion. Develops required specifications for simple to moderately complex systems. Assists senior computer systems analyst in preparing input and test data for the proposed system.

14. Systems Analyst 2

Education: Bachelors or equivalent in professional experience.
General Experience: Three years of independent professional work, including responsibility for performing independent project-level tasks under relatively close supervision and monitoring.

Duties: Typically serves as programmer, engineer, systems analyst, training specialist, database administrator, technical writer, configuration manager, technician, LAN administrator, or graphics artist. Supports day-to-day project operations. Performs assigned tasks that are varied and somewhat difficult in character. Instructions are typically broad and general in nature.

15. Systems Analyst 3

Education: Masters or equivalent in professional experience.
General Experience: Six years of technical leadership, including independent project responsibility plus responsibility for assisting at the decision-making level in major program operations. Must have served as key technical resource for the customer.

Duties: Typically serves as principal data analyst, principal systems engineer, principal programmer, principal configuration manager, principal technical write, principal resource planner, or principal database administrator. Performs varied and difficult tasks under minimum supervision, conferring with supervisor on unusual matters. May be assisted by or may supervise more junior personnel. Has some latitude for unsupervised decision and action.

16. Systems Analyst 4

Education: Masters or equivalent in professional experience.
General Experience: Ten years of management experience including major program-level responsibilities under only policy guidance and general supervision. Must have demonstrated the ability to serve as technical lead interface with the customer.

Duties: Typically serves as project manager, senior data analyst, senior systems engineer, senior programmer, senior configuration manager, or senior technical writer. May plan, conduct, supervise, and/or manage most tasks under minimum supervision, conferring with the supervisor on unusual matters. Assignments are broad in nature, requiring originality and ingenuity. May train or supervise junior and mid-level staff. Has substantial latitude for unsupervised decision and action. May have overall responsibility for project financial and technical management.

17. Database Manager

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 6 years of experience in the development and/or maintenance of database systems, including 4 years of specialized experience.

Specialized Experience: At least 4 years of experience with database management systems, system design and analysis, operating systems software, and internal and data manipulation languages.

Duties: Must be capable of managing the development of database projects. Plans and budgets staff and data resources. Supports application developers in planning preparation, load analysis, and back-up and recovery of data. When necessary, reallocates resources to maximize benefits. Prepares and delivers

presentations on DBMS concepts. Provides daily supervision and direction to support staff. Monitors performance and evaluates areas to improve efficiency.

18. Software Engineer

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 3 years of experience as a software engineer, including 2 years of specialized experience.

Specialized Experience: At least 2 years of experience working with third- or fourth- generation languages in the design and implementation of systems and 1-year working with DBMSs.

Duties: Reviews and analyzes system specifications. Prepares programming specifications. Analyzes existing systems/subsystems for reusability benefits and needed changes. Prepares design plans and written analyses. Prepares unit and test scripts. Prepares documentation. Applications include the full range of management information systems, weapons systems, and Year 2000 solutions.

19. Research Analyst

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 5 years of experience in defining and formulating models, including 3 years of specialized experience.

Specialized Experience: At least 3 years of experience in operations research related directly to economic analysis, cost modeling, and modeling ADP problems.

Duties: Must be able to apply appropriate operations research modeling techniques to problems that model input, output, and logical flow in sufficient detail for programming. Monitors the mathematical and programming aspects of a project for adherence to the objectives of the model. Develops models that can utilize simulation. Applies operations research methodology to define and formulate economic analysis and related benefit, cost, and risk studies. Must have knowledge of principles, theories, procedures, and techniques of cost analysis, including statistical concepts, financial analysis concepts, and cost accounting concepts

20. Communications Network Manager

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 5 years of experience in all aspects of communication networks planning, installation, and support, including 3 years of specialized experience.

Specialized Experience: At least 3 years of experience in the supervision of operations and maintenance activities for voice and data communications networks. Specialized experience also includes protocol analysis and knowledge of LAN and WAN data communications protocols, including but not limited to TCP/IP, ATM, frame relay, X.400, X.500. Experience with bridges, routers, gateways, Fiber Distributed Data Interface (FDDI), and UNIX operating systems. Experience as a CNE or ECNE desirable.

Duties: Evaluates communication hardware and software, troubleshoots LAN/MAN/WAN and other network-related problems, and provides technical expertise for performance and configuration of networks. Performs and supervises general voice and data network administration, and provides technical leadership in the integration and test of complex large-scale networks. Schedules network conversions and cutovers. Oversees network control center. Supervises maintenance of network systems, including PBXs, ACDs, routers, bridges, multiplexers, LAN hubs, and ATM switches. Coordinates with all responsible users and sites. Supervises staff.

21. Security Systems Specialist 1

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 5 years of experience in computer security systems, including 2 years of specialized experience.
Specialized Experience: At least 2 years of experience in defining computer security requirements for high-level applications, evaluating approved security product capabilities, and developing solutions to MLS problems.

Duties: Analyzes and defines security requirements for MLS issues. Designs, develops, engineers, and implements solutions to MLS requirements. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena. Performs risk analyses, which also include risk assessment

22. Security Systems Specialist 2

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 8 years of experience with computer security systems, including 4 years of specialized experience.

Specialized Experience: At least 4 years of experience in defining computer security requirements for high-level applications, evaluation of approved security product capabilities, and developing solutions to Multilevel Security (MLS) problems.

Duties: Analyzes and defines security requirements for MLS issues. Designs, develops, engineers, and implements solutions to MLS requirements. Responsible for the implementation and development of the MLS. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena. Performs risk analyses, which also include risk assessment. Provides daily supervision and direction to staff.

23. Documentation Specialist

Education: Associate's degree or equivalent experience in a related field.
General Experience: Must have 2 years of experience in technical writing, and documentation experience pertaining to all aspects of ADP, including 2 years of specialized experience.

Specialized Experience: A minimum of 2 years of experience in preparing technical documentation, including research for applicable standards.

Duties: Gathers, analyzes, and composes technical information. Conducts research and ensures the use of proper technical terminology. Translates technical information into clear, readable documents to be used by technical and nontechnical personnel. For applications built to run in a Windows environment, uses the standard help compiler to prepare all on-line documentation

24. Consultant

Education: B.A. or B.S. degree or equivalent experience in a related field.
Specialized Experience: Possesses a high level of specialized expertise in a particular subject matter area and/or technology. Provides consulting to directors and senior managers on quality improvement. Develops, leads, and conducts quality workshops, benchmarking, and surveys. Facilitates process improvement efforts. Manages a team of consultants and analysts. Generates papers and documents.

25. Engineer 1

Education: B.S. degree or equivalent experience in a related field.
General Experience: Must have 4 years of engineering experience. Additional education may be substituted for years of experience.

Specialized Experience: At least 2 years of experience as an engineer in support of telecommunications, system installation, data automation, or a related field.

Duties: Applies knowledge of and experience with engineering principles and techniques in the design, development, installation, integration, analysis, operation, maintenance, testing, and evaluation of software and ADP, security, telecommunications, or supervisory control, and data acquisition systems related projects and programs.

26. Engineer 2

Education: B.S. degree or equivalent experience.
General Experience: Must have 6 years of engineering experience. Additional education may be substituted for years of experience.

Specialized Experience: At least 3 years of experience as an engineer in support of telecommunications, system installation, data automation, or a related field.

Duties: Applies knowledge of and experience with engineering principles and techniques in the design, development, installation, integration, analysis, operation, maintenance, testing, and evaluation of software and ADP, security, telecommunications, or supervisory control, and data acquisition systems related projects and programs. Provides these functions with little to no supervision. May supervise other engineers.

27. Engineer 3

Education: B.S. degree or equivalent experience.
General Experience: Must have 8 years of engineering experience. Additional education may be substituted for years of experience.

Specialized Experience: At least 4 years of experience as an engineer in support of telecommunications, system installation, data automation, or a related field.

Duties: Applies knowledge of and experience with engineering principles and techniques in the design, development, installation, integration, analysis, operation, maintenance, testing, and evaluation of software and ADP, security, telecommunications, or supervisory control, and data acquisition systems related projects and programs. Provides these functions with no supervision. May supervise other engineers or teams of engineers.

28. Administrative Support Analyst/Specialist

Education: HS diploma or equivalent experience.
General Experience: Must have 1 year of experience working in an automated office environment. No specialized experience is required.

Duties: To produces, maintains, and updates documents, reports, and correspondence utilizing a word processing system or computer word processing software. May develop processes to maintain, track, and distribute documents in support of engineers, analysts, specialists, or programmers. May support the selection of office automation hardware and software

29. Information Assurance Engineer 1

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 10 years of experience in managing the implementation of information engineering projects and experience in systems analysis, design, and programming, including 5 years of specialized experience.

Specialized Experience: At least 5 years of experience in information systems development, functional and data requirements analysis, systems analysis and design, programming, program design, and documentation preparation.

Duties: Must be capable of applying enterprise-wide set of disciplines for planning, analysis, design, and construction of information systems on an enterprise-wide basis or across a major sector of the enterprise. Develops analytical and computational techniques and methodology for problem solutions. Performs enterprise-wide strategic systems planning, information planning, business, and analysis. Performs process and data modeling in support of the planning and analysis efforts using manual and automated tools, such as Integrated Computer-Aided Software Engineering (I-CASE) tools. Must be able to apply reverse engineering and reengineering disciplines to develop migration strategic and planning documents. Provides technical guidance in software engineering techniques and automated support tools.

30. Information Assurance Engineer 2

Education: B.S. degree or equivalent experience in a related field.
General Experience: Must have 10 years of Information Assurance experience including 6 years of specialized experience. Must be able to obtain a security clearance at the TS/SCI level. Additional education may be substituted for years of experience.

Specialized Experience: At least 7 years experience as an engineer in support of telecommunications, system installation, data automation, or a related field. Expert in the application of information assurance, engineering principles and techniques in the secure design, development, integration, analysis, operation, maintenance, testing, and evaluation of software and ADP, security, telecommunications, or supervisory control, and data acquisition systems related projects and programs. May supervise other engineers or teams of engineers.

31. Intelligence Analyst 1

Education: B.A. degree or equivalent experience in a related field.
General Experience: Must have some knowledge of Intelligence Analysis and be able to obtain a security clearance at the TS/SCI level. Additional education may be substituted for level of experience.

Specialized Experience: Under direction, conduct intelligence-related research on well-established topics in support of a larger analytical effort from both classified and unclassified data. Compile and organize data for senior analyst in response to assigned taskings of increasing complexity including the entry of data into a database system. Maintain data files and conduct searches to provide information as part of more in-depth analytical taskings. Identify basic intelligence gaps and provide input to the formulation of collected sources. Perform basic analysis by correlating data from a limited number of sources. Provide limited assessments to more senior intelligence analysts and recommend conclusions and findings. Identify and use established or directed techniques and methodologies. Provide input regarding project and workload planning to senior analysts and supervisors. Follow basic security guidelines and procedures. Prepare, produce, and disseminate scheduled and unscheduled intelligence products limited in

scope and complexity. Also, contribute to major intelligence studies. Analysts at this level likely require regular coaching, mentoring, training, and assistance from others.

32. Intelligence Analyst 2

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 4 years of Intelligence Analysis experience and be able to obtain a security clearance at the TS/SCI level. Additional education may be substituted for years of experience.

Specialized Experience: Conduct comprehensive related research on complex topics either independently or as part of a larger analytical effort. Serve as a project leader directing the research efforts of more junior analysts. Determine research methodology and work approach and revise as appropriate. Ensure integrity of databases and compare and contrast information from different sources. Modify and create necessary data files and manipulate data to develop responses to a wide range of complex, all-source intelligence taskings; evaluate correctness/accuracy of researched material. Prepare detailed specifications for collection or change to standing requirements based on knowledge of collection systems. Assess progress of research efforts and redirect efforts of teams as necessary. Provide on-the-job training and substantive guidance to lower- graded analyst on all aspects of work. Plan work approach for projects. Delineate and prioritize tasks for junior analysts. Identify resource requirements and shortfalls to supervisor. Ensure implementation of security guidelines procedures. Review projects for compliance. Interpret more complex security policy. Prepare, produce, and disseminate both scheduled and unscheduled general military intelligence products, such as: briefings, studies, estimates, and assessments memoranda. Identify target audience for products. Represent activity in working groups and committees as substantive authority in subject area. Initiate analytical contacts to enhance mission effectiveness. Be prepared to represent activity at national and international forums. Analyst at this level can perform independently much of the time, and require coaching, mentoring and /or assistance only in difficult or unusual situations.

33. Intelligence Analyst 3

Education: B.A. or B.S. degree or equivalent experience in a related field.
General Experience: Must have 7 years of Intelligence Analysis experience and be able to obtain a security clearance at the TS/SCI level. Additional education may be substituted for years of experience.

Specialized Experience: Define critical intelligence topics and initiate comprehensive or unique research efforts on topics as related to extensive or speculative analytical projects. Oversees team efforts insuring proper utilization of methodologies and approaches across the teams. Identify requirements for new databases and information services, and develop new research methodologies. Define overall analytical objectives in relation to existing or proposed policy and identify required analytical resources. Forecast intelligence gaps and initiate development of comprehensive collection plans to address these gaps. Perform long-range planning in support of existing and projected organizational mission requirements. Make assessments as to overall resource capability to answer existing/projected requirements, and identify resource shortfalls. Evaluate impact of security policy on organization effectiveness. In addition to the production and dissemination of the product at the Intelligence analyst level, Senior Analysts evaluate the most complex, sensitive intelligence products and insure other substantive accuracies. Recommend most effective product type and format for dissemination of initial intelligence. Analysts at this level require little or no coaching or assistance and, in fact, assist and mentor others regularly. They can successfully manage difficult or unusual situations on their own.

34. Intelligence Analyst 4

Education: B.A. or B.S. Degree or equivalent experience in related field. M.A. degree or foreign language desired.
General Experience: Must have 10 years of Intelligence Analysis experience including 6 years of specialized experience. Must be able to obtain a security clearance at the TS/SCI level. Additional education may be substituted for years of experience.

Specialized Experience: Intelligence Analyst or functional expert, exceptionally qualified, by experience or education, in a specified technical or regional area. Conduct comprehensive related research on complex topics either independently or as part of a larger analytical effort. Serve as a project leader directing the research efforts of more junior analysts. Determine research methodology and work approach and revise as appropriate. Ensure integrity of databases and compare and contrast information from different sources. Modify and create necessary data files and manipulate data to develop responses to a wide range of complex, all-source intelligence taskings; evaluate correctness/accuracy of researched material. Prepare detailed specifications for collection or change to standing requirements based on knowledge of collection systems. Assess progress of research efforts and redirect efforts of teams as necessary. Provide on-the-job training and substantive guidance to lower-graded analyst on all aspects of work. Plan work approach for projects. Delineate and prioritize tasks for junior analysts. Identify resource requirements and shortfalls to supervisor. Ensure implementation of security guidelines procedures. Review projects for compliance. Interpret more complex security policy. Prepare, produce, and disseminate both scheduled and unscheduled general military intelligence products, such as: briefings, studies, estimates, and assessments memoranda. Identify target audience for products. Represent activity in working groups and committees as substantive authority in subject area. Initiate analytical contacts to enhance mission effectiveness. Be prepared to represent activity at national and international forums. Analysts at this level perform independently, and require mentoring and /or assistance from senior management in only exceptionally difficult or unusual situations.

35. Information Systems Security (INFOSEC) Analyst 1

Education: B.A. or B.S. degree.
General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, INFOSEC, engineering, math, physics, or a closely related field. Analysts must demonstrate technical experience in electronic commerce, information system architecture development and design, physical security, personnel security, contingency or continuity of operations planning, quality assurance, configuration management, systems analysis, or information systems management. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: INFOSEC Analyst works on complex system and management problems involving all phases of information systems analysis to provide INFOSEC solutions. Analysts provide technical support for development and review of INFOSEC management procedures, INFOSEC product analysis and studies, risk management, and support for secure software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards. The INFOSEC Analyst applies knowledge of current INFOSEC policy and the national INFOSEC structure to provide recommendations for INFOSEC policy and procedures at all levels of government. INFOSEC Analysts review and recommend INFOSEC solutions to customer problems based on an understanding of how products and services interrelate and support the INFOSEC mission. The INFOSEC Analyst recommends resolution of INFOSEC problems based on knowledge of the major INFOSEC products and services, an understanding of their limitations, and a working knowledge of the disciplines of INFOSEC. Analysts generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate

36. Information Systems Security (INFOSEC) Analyst 2

Education: B.A. or B.S. degree and 5 years minimum equivalent experience in a related field.
General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, INFOSEC, engineering, math, physics, or a closely related field. Analysts must demonstrate technical experience in electronic commerce, information system architecture development and design, physical security, personnel security, contingency or continuity of operations planning, quality assurance, configuration management, systems analysis, or information systems management. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: INFOSEC Analyst works on complex system and management problems involving all phases of information systems analysis to provide INFOSEC solutions. Analysts provide technical support for development and review of INFOSEC management procedures, INFOSEC product analysis and studies, risk management, and support for secure software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards. The INFOSEC Analyst applies knowledge of current INFOSEC policy and the national INFOSEC structure to provide recommendations for INFOSEC policy and procedures at all levels of government. INFOSEC Analysts review and recommend INFOSEC solutions to customer problems based on an understanding of how products and services interrelate and support the INFOSEC mission. The INFOSEC Analyst recommends resolution of INFOSEC problems based on knowledge of the major INFOSEC products and services, an understanding of their limitations, and a working knowledge of the disciplines of INFOSEC. Analysts generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate.

37. Information Systems Security (INFOSEC) Analyst 3

Education: B.A. or B.S. degree and 7 years minimum equivalent experience in a related field.
General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, INFOSEC, engineering, math, physics, or a closely related field. Analysts must demonstrate technical experience in electronic commerce, information system architecture development and design, physical security, personnel security, contingency or continuity of operations planning, quality assurance, configuration management, systems analysis, or information systems management. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: INFOSEC Analyst works on complex system and management problems involving all phases of information systems analysis to provide INFOSEC solutions. Analysts provide technical support for development and review of INFOSEC management procedures, INFOSEC product analysis and studies, risk management, and support for secure software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards. The INFOSEC Analyst applies knowledge of current INFOSEC policy and the national INFOSEC structure to provide recommendations for INFOSEC policy and procedures at all levels of government. INFOSEC Analysts review and recommend INFOSEC solutions to customer problems based on an understanding of how products and services interrelate and support the INFOSEC mission. The INFOSEC Analyst recommends resolution of INFOSEC problems based on knowledge of the major INFOSEC products and services, an understanding of their limitations, and a working knowledge of the disciplines of INFOSEC. Analysts generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate.

38. Information Systems Security (INFOSEC) Analyst 4

Education: B.A. or B.S. degree and 10 years minimum equivalent experience in a related field.
General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, INFOSEC, engineering, math, physics, or a closely related field. Analysts must demonstrate technical experience in electronic commerce, information system architecture development and design, physical security, personnel security, contingency or continuity of operations planning, quality assurance, configuration management, systems analysis, or information systems management. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: INFOSEC Analyst works on complex system and management problems involving all phases of information systems analysis to provide INFOSEC solutions. Analysts provide technical support for development and review of INFOSEC management procedures, INFOSEC product analysis and studies, risk management, and support for secure software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards. The INFOSEC Analyst applies knowledge of current INFOSEC policy and the national INFOSEC structure to provide recommendations for INFOSEC policy and procedures at all levels of government. INFOSEC Analysts review and recommend INFOSEC solutions to customer problems based on an understanding of how products and services interrelate and support the INFOSEC mission. The INFOSEC Analyst recommends resolution of INFOSEC problems based on knowledge of the major INFOSEC products and services, an understanding of their limitations, and a working knowledge of the disciplines of INFOSEC. Analysts generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate.

39. INFOSEC Engineer 1

Education: B.A. or B.S. degree and 10 years minimum equivalent experience in a related field.
General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, INFOSEC, engineering, math, physics, or a closely related field. These staff have demonstrated specific experience in one or more of the technical INFOSEC functional engineering areas: Computer Security (COMPUSEC), Communications Security (COMSEC), TEMPEST, or Operations Security (OPSEC). Engineers demonstrate experience in analytical problem solving involving systems design and integration, system analysis and testing, independent verification and validation (IV&V), or risk analysis and have demonstrated experience with INFOSEC products and systems. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: INFOSEC Engineers provide the expertise to conduct INFOSEC systems analysis, certification and accreditation, integration of secure products, security test and evaluation (ST&E), or development of complex information systems that will meet the assigned INFOSEC requirements. INFOSEC Engineers demonstrate a broad knowledge of the technical INFOSEC discipline and apply extensive expertise as an information engineering professional. Engineers generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate.

40. INFOSEC Engineer 2

Education: B.A. or B.S. degree and 20 years minimum equivalent experience in a related field.

General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, INFOSEC, engineering, math, physics, or a closely related field. These staff have demonstrated specific experience in one or more of the technical INFOSEC functional engineering areas: Computer Security (COMPUSEC), Communications Security (COMSEC), TEMPEST, or Operations Security (OPSEC). Engineers demonstrate experience in analytical problem solving involving systems design and integration, system analysis and testing, independent verification and validation (IV&V), or risk analysis and have demonstrated experience with INFOSEC products and systems. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: INFOSEC Engineers provide the expertise to conduct INFOSEC systems analysis, certification and accreditation, integration of secure products, security test and evaluation (ST&E), or development of complex information systems that will meet the assigned INFOSEC requirements. INFOSEC Engineers demonstrate a broad knowledge of the technical INFOSEC discipline and apply extensive expertise as an information engineering professional. Engineers generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate.

41. INFOSEC Engineer 3

Education: Masters degree and 10 years minimum equivalent experience in a related field.
General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, INFOSEC, engineering, math, physics, or a closely related field. These staff have demonstrated specific experience in one or more of the technical INFOSEC functional engineering areas: Computer Security (COMPUSEC), Communications Security (COMSEC), TEMPEST, or Operations Security (OPSEC). Engineers demonstrate experience in analytical problem solving involving systems design and integration, system analysis and testing, independent verification and validation (IV&V), or risk analysis and have demonstrated experience with INFOSEC products and systems. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: INFOSEC Engineers provide the expertise to conduct INFOSEC systems analysis, certification and accreditation, integration of secure products, security test and evaluation (ST&E), or development of complex information systems that will meet the assigned INFOSEC requirements. INFOSEC Engineers demonstrate a broad knowledge of the technical INFOSEC discipline and apply extensive expertise as an information engineering professional. Engineers generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate.

42. INFOSEC Engineer 4

Education: PHD degree and 15 years minimum equivalent experience in a related field.
General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, INFOSEC, engineering, math, physics, or a closely related field. These staff have demonstrated specific experience in one or more of the technical INFOSEC functional engineering areas: Computer Security (COMPUSEC), Communications Security (COMSEC), TEMPEST, or Operations Security (OPSEC). Engineers demonstrate experience in analytical problem solving involving systems design and integration, system analysis and testing, independent verification and validation (IV&V), or risk analysis and have demonstrated experience with INFOSEC products and systems. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: INFOSEC Engineers provide the expertise to conduct INFOSEC systems analysis, certification and accreditation, integration of secure products, security test and evaluation (ST&E), or development of complex information systems that will meet the assigned INFOSEC requirements. INFOSEC Engineers demonstrate a broad knowledge of the technical INFOSEC discipline and apply extensive expertise as an information engineering professional. Engineers generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate.

43. Managed Security Engineer

Education: B.A. or B.S. degree and 2 years minimum equivalent experience in a related field.
General Experience: Managed Security Engineers (MSEs) must possess professional training or equivalent experience in one or more of the following types of disciplines: security operations / network operations; Firewall, VPN, and IDS devices; network management; multiple operating systems (UNIX, Win32); internal / external assessments; and device configuration, design and integration. MSEs must have demonstrated skills in analytical problem solving and the ability to conduct event analysis and risk mitigation procedures. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: MSEs perform a variety of functions related to the day-to-day operations of a 24x7 Network Security Operations Center (NSOC). MSEs are responsible for traffic monitoring, network performance and integrity, and contingency and disaster recovery planning for Managed Security Services. MSEs provide customer support and document security incidents while troubleshooting support of deployed Firewalls, Virtual Private Networks (VPNs), and Intrusion Detection devices. MSEs participate in Computer Incident Response Teams to conduct forensics and restore customers' IT systems. Duties include provisioning, maintenance and assisting in optimizing all NSOC incident handling and escalation procedures.

44. Systems Security Architect 1

Education: Associate degree and 3 years minimum equivalent experience in a related field.
General Experience: Systems Security Architects (SSAs) must possess significant expertise in one or more of the following types of disciplines: designing, developing and implementing technical IT security programs; conducting security assessments and designing architectures; experience and solid understanding of enterprise, system, network, and application security issues including TCP/IP, firewalls, intrusion detection devices, encryption, and VPNs; system / database administration; multiple operating systems (UNIX, NT, W2000, Mainframes); Public Key Infrastructure; database and transactional security; application source code; and user identification, authentication and auditing. SSAs must have demonstrated skills in analytical problem solving involving system design and integration and have demonstrated experience with security products and systems. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: SSAs assume leadership roles in developing, implementing, and maintaining enterprise-wide information security capabilities. SSAs analyze the enterprise business models, Information Technology (IT) needs, long range plan, and existing IT systems to determine business security risks and risk management considerations. The SSAs define appropriate enterprise and system level security requirements. SNAs evaluate and/or propose technical solutions for systems and applications-level security architecture and design and ensure the solutions are validated. SNAs tasks include developing and evaluating security plans, policies, procedures and practices. Duties include

assessing the quality and viability of solution architectures, design integrity and the required interfaces with internal and external systems.

45. Systems Security Architect 2

Education: Associate degree and 3 years minimum equivalent experience in a related field.

General Experience: Systems Security Architects (SSAs) must possess significant expertise in one or more of the following types of disciplines: designing, developing and implementing technical IT security programs; conducting security assessments and designing architectures; experience and solid understanding of enterprise, system, network, and application security issues including TCP/IP, firewalls, intrusion detection devices, encryption, and VPNs; system / database administration; multiple operating systems (UNIX, NT, W2000, Mainframes); Public Key Infrastructure; database and transactional security; application source code; and user identification, authentication and auditing. SSAs must have demonstrated skills in analytical problem solving involving system design and integration and have demonstrated experience with security products and systems. Must be able to obtain a security clearance at the TS/SCI level. Additional experience may be substituted for education requirements.

Specialized Experience: SSAs assume leadership roles in developing, implementing, and maintaining enterprise-wide information security capabilities. SSAs analyze the enterprise business models, Information Technology (IT) needs, long range plan, and existing IT systems to determine business security risks and risk management considerations. The SSAs define appropriate enterprise and system level security requirements. SNAs evaluate and/or propose technical solutions for systems and applications-level security architecture and design and ensure the solutions are validated. SNAs tasks include developing and evaluating security plans, policies, procedures and practices. Duties include assessing the quality and viability of solution architectures, design integrity and the required interfaces with internal and external systems.

46. DoD 8570 Information Assurance Technical (IAT) Level 1
Performs all the functions and responsibilities required per *DoD Directive 8570.01-M*

47. DoD 8570 Information Assurance Technical (IAT) Level 2
Performs all the functions and responsibilities required per *DoD Directive 8570.01-M*

48. DoD 8570 Information Assurance Technical (IAT) Level 3
Performs all the functions and responsibilities required per *DoD Directive 8570.01-M*

49. DoD 8570 Information Assurance Management (IAM) Level 1
Performs all the functions and responsibilities required per *DoD Directive 8570.01-M*

50. DoD 8570 Information Assurance Management (IAM) Level 2
Performs all the functions and responsibilities required per *DoD Directive 8570.01-M*.

51. DoD 8570 Information Assurance Management (IAM) Level 3
Performs all the functions and responsibilities required per *DoD Directive 8570.01-M*

See Notes Pertaining to Categories 46 – 51 on the following page.

Information Assurance Technical (IAT) and IA Management (IAM) personnel must be fully trained and certified to baseline requirements to perform their IA duties. The policy defines IAT workforce members as anyone with privileged information system access performing IA functions. IAM personnel perform management functions for DoD operational systems described in the Manual (DoD 8570.01-M).

Individuals in IA positions, as defined in Chapters 3, 4, 5, 10, and 11 of the Manual not meeting certification requirements must be reassigned to other duties, consistent with applicable law. Until certification is attained, individuals in IA positions not meeting certification requirements may perform those duties under the direct supervision of an appropriately certified individual unless the certification requirement has been waived due to severe operational or personnel constraints. (See paragraphs C3.2.4.2., C3.2.4.3., C.4.2.3.2.1., C4.2.3.4.2., C10.2.3.4., and C11.2.4.2.)

The DoD Directive/Manual is subject to change. A current version can be found at www.dtic.mil

Labor Rates

Period: 10/21/2010 to 10/20/2011**

Note that discounted labor rates may be available based on customer requirements.

	Labor Category	GSA Government Site Rate	GSA BAE Site Rate		Labor Category	GSA Government Site Rate	GSA BAE Site Rate
1	Program Manager	$159.52	$180.89	27	Engineer - 3	$128.23	$145.41
2	Project Manager	$129.80	$147.20	28	Admin. Support Analyst/Specialist	$45.34	$51.41
3	Software/Integration Analyst	$104.79	$118.84	29	Information Assurance Engineer - 1	$139.20	$157.85
4	Subject Matter Expert - 1	$134.47	$152.49	30	Information Assurance Engineer - 2	$214.59	$243.36
5	Subject Matter Expert - 2	$165.76	$187.97	31	Intelligence Analyst - 1	$81.15	$92.02
6	Process Re-Engineering Spec. - 1	$115.71	$131.21	32	Intelligence Analyst - 2	$114.18	$129.47
7	Process Re-Engineering Spec. - 2	$148.57	$168.47	33	Intelligence Analyst - 3	$136.19	$154.44
8	Computer Specialist - 1	$65.67	$74.47	34	Intelligence Analyst - 4	$182.96	$207.47
9	Computer Specialist - 2	$75.06	$85.13	35	INFOSEC Analyst Level - 1	$62.09	$70.42
10	Project Control - 1	$59.42	$67.38	36	INFOSEC Analyst Level - 2	$89.43	$101.41
11	Project Control - 2	$84.45	$95.77	37	INFOSEC Analyst Level - 3	$99.19	$112.50
12	Project Control - 3	$106.34	$120.58	38	INFOSEC Analyst Level - 4	$132.90	$150.72
13	Systems Analyst - 1	$67.26	$76.26	39	INFOSEC Engineer Level - 1	$149.05	$169.03
14	Systems Analyst - 2	$79.79	$90.47	40	INFOSEC Engineer Level - 2	$160.78	$182.33
15	Systems Analyst - 3	$113.50	$128.70	41	INFOSEC Engineer Level - 3	$177.06	$200.79
16	Systems Analyst - 4	$147.20	$166.93	42	INFOSEC Engineer Level - 4	$195.34	$221.52
17	Database Manager	$101.67	$115.28	43	Managed Security Engineer	$271.90	$308.34
18	Software Engineer	$70.39	$79.83	44	Systems Security Architect - 1	$271.91	$308.36
19	Research Analyst	$84.45	$95.77	45	Systems Security Architect - 2	$339.89	$385.43
20	Communications Network Manager	$82.87	$93.98	46	DoD IAM - 1	$100.47	$110.01
21	Security Systems Specialist - 1	$68.81	$78.03	47	DoD IAM - 2	$116.97	$128.08
22	Security Systems Specialist - 2	$90.71	$102.86	48	DoD IAM - 3	$138.46	$151.60
23	Documentation Specialist	$54.75	$62.09	49	DoD IAT - 1	$60.94	$66.72
24	Consultant	$312.77	$354.68	50	DoD IAT - 2	$89.35	97.83
25	Engineer - 1	$81.34	$92.23	51	DoD IAT - 3	$106.33	$116.43
26	Engineer - 2	$107.92	$122.37				

**** Rates for years beyond 2011 will be negotiated prior to 10/20/2011with pricing updates applied to this pricelist.**